(12) UK Patent Application (19) GB (11) 2 297 016 (13) A

(43) Date of A Publication 17.07.1996

(21) Application No 9525817.4

(22) Date of Filing 18.12.1995

(30) Priority Data
(31) 0718819 (32) 12.01.1995 (33) JP

(71) Applicant(s)
Kokusai Denshin Denwa Co Ltd

(Incorporated in Japan)

3-2 Nishi-Shinjuku 2-chome, Shinjuku-ku, Tokyo, Japan

(72) Inventor(s)
Masayoshi Ohashi
Seiichiro Sakai
Toshinori Suzuki

(74) Agent and/or Address for Service
Gill Jennings & Every
Broadgate House, 7 Eldon Street, LONDON, EC2M 7LH, United Kingdom

(51) INT CL[6]
H04L 9/30

(52) UK CL (Edition O)
H4P PDCSC

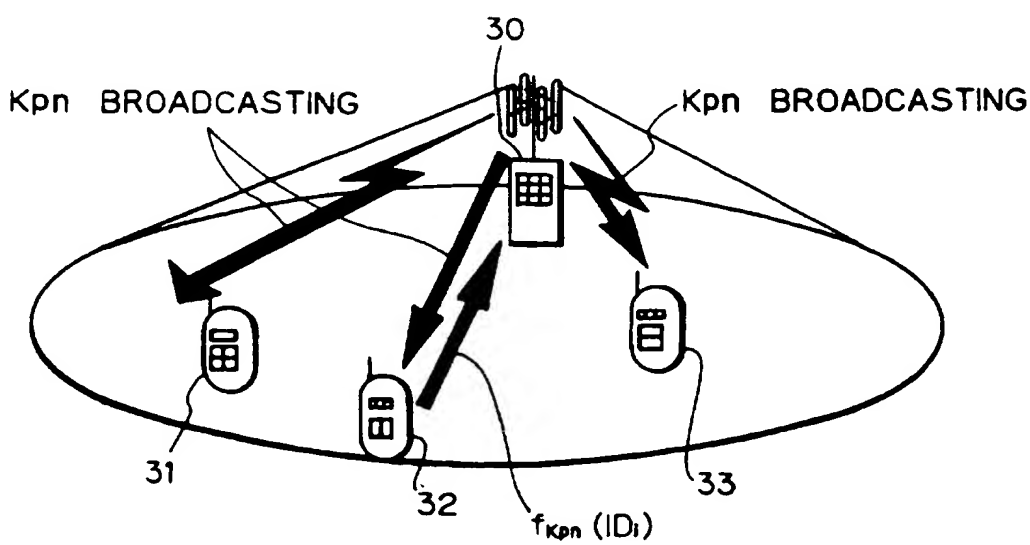
(56) Documents Cited
US 5222140 A

(58) Field of Search
UK CL (Edition O) H4P PDCSA PDCSC
INT CL[6] H04L 9/30 9/32
Online:WPI, Claims, Inspec

(54) **Identity confidentiality using public key encryption in radio communication**

(57) The radio communication system has at least one first radio station such as a base station (30) and a plurality of second radio stations such as mobile stations (31 - 33). The base station (30) at least possesses a public key, and each of the mobile stations (31 - 33) possesses a public-key cryptography function for ciphering the public key and an identity for identifying itself. An identity confidentiality method includes steps of generating a time-varying public key at the base station, and repeatedly broadcasting, from the base station, the generated time-varying public key to all the mobile stations so that the mobile stations can cipher the respective identities with the broadcasted time-varying public key.

Fig. 3



GB 2 297 016 A

Fig. 1

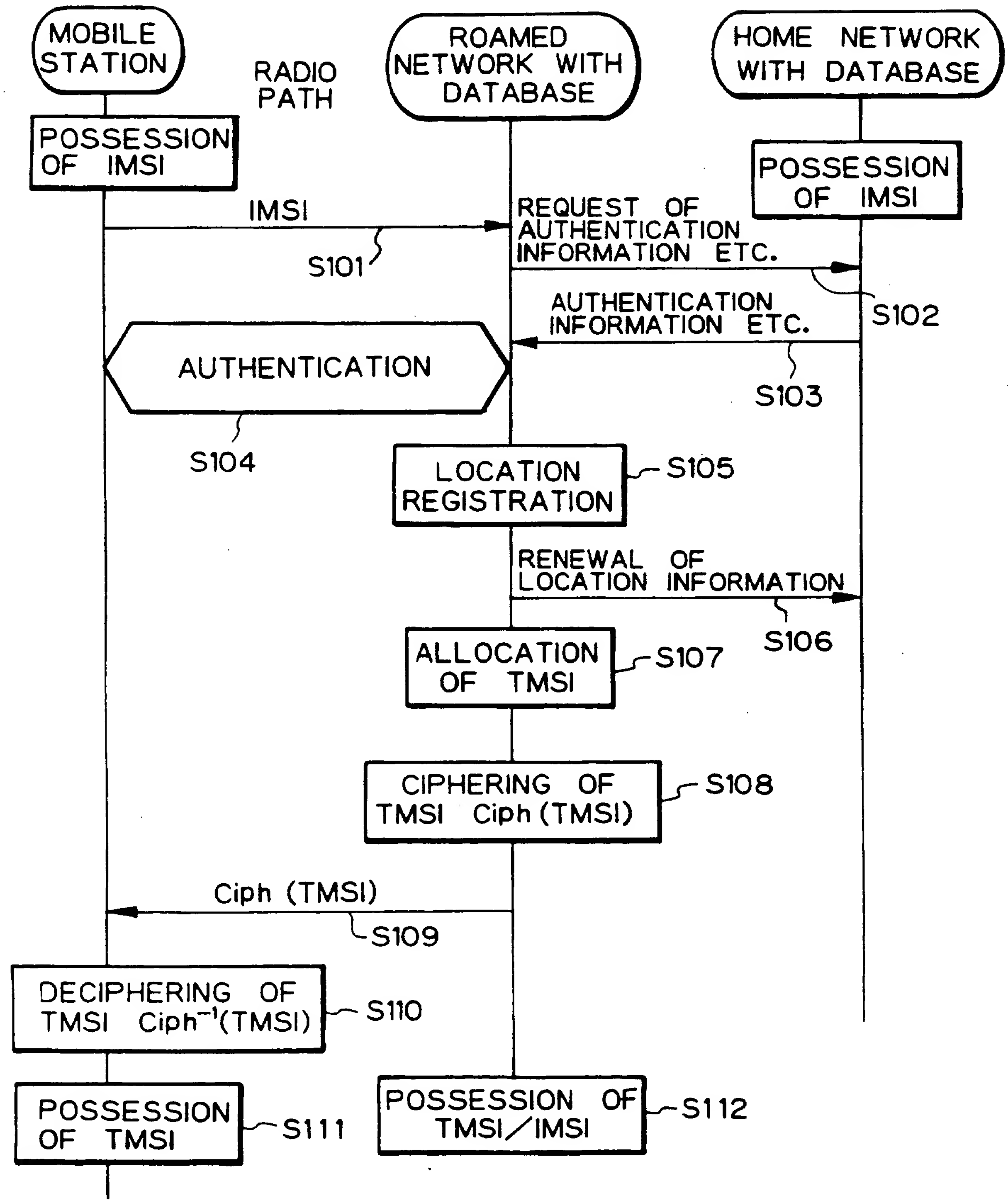

MOBILE STATION
RADIO PATH
ROAMED NETWORK WITH DATABASE
HOME NETWORK WITH DATABASE
POSSESSION OF IMSI
POSSESSION OF IMSI
IMSI
S101
REQUEST OF AUTHENTICATION INFORMATION ETC.
S102
AUTHENTICATION INFORMATION ETC.
S103
AUTHENTICATION
S104
LOCATION REGISTRATION
S105
RENEWAL OF LOCATION INFORMATION
S106
ALLOCATION OF TMSI
S107
CIPHERING OF TMSI Ciph (TMSI)
S108
Ciph (TMSI)
S109
DECIPHERING OF TMSI Ciph⁻¹(TMSI)
S110
POSSESSION OF TMSI
S111
POSSESSION OF TMSI/IMSI
S112

Fig. 2

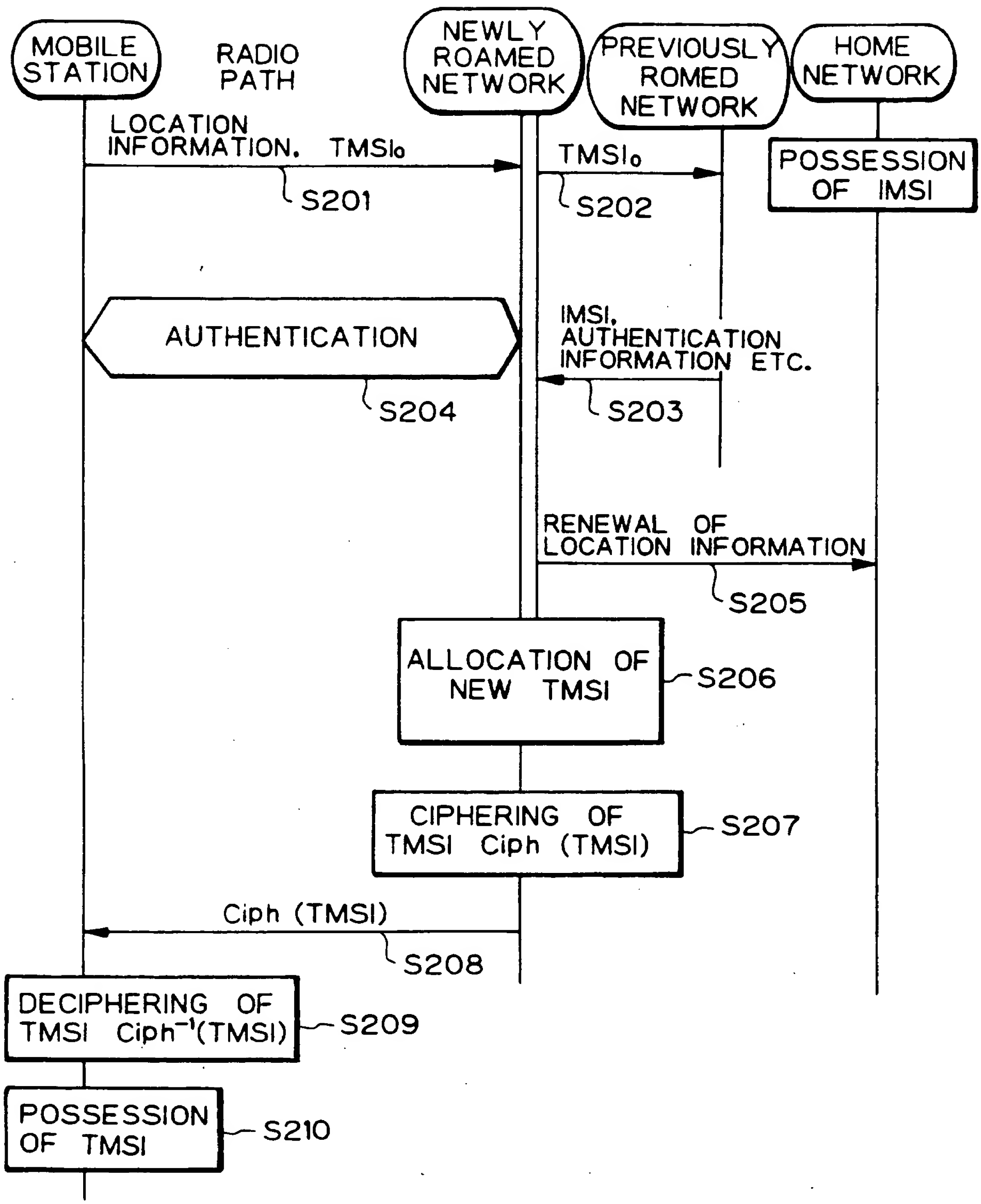

MOBILE STATION
RADIO PATH
NEWLY ROAMED NETWORK
PREVIOUSLY ROMED NETWORK
HOME NETWORK
LOCATION INFORMATION. TMSI0
S201
TMSI0
S202
POSSESSION OF IMSI
AUTHENTICATION
S204
IMSI, AUTHENTICATION INFORMATION ETC.
S203
RENEWAL OF LOCATION INFORMATION
S205
ALLOCATION OF NEW TMSI
S206
CIPHERING OF TMSI Ciph (TMSI)
S207
Ciph (TMSI)
S208
DECIPHERING OF TMSI Ciph⁻¹(TMSI)
S209
POSSESSION OF TMSI
S210

Fig. 3

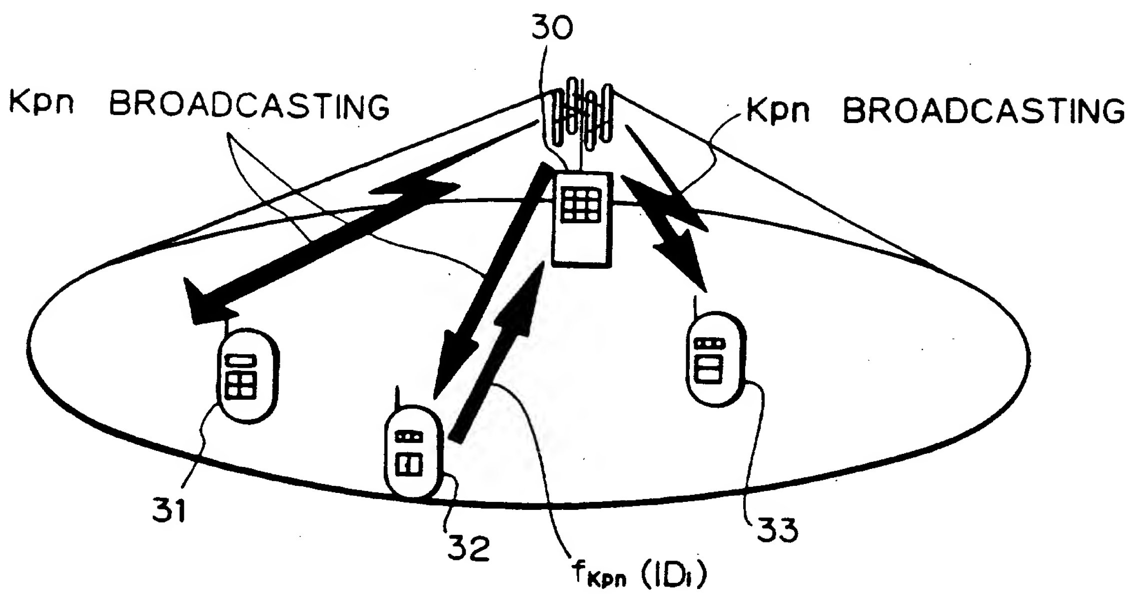


Fig. 4

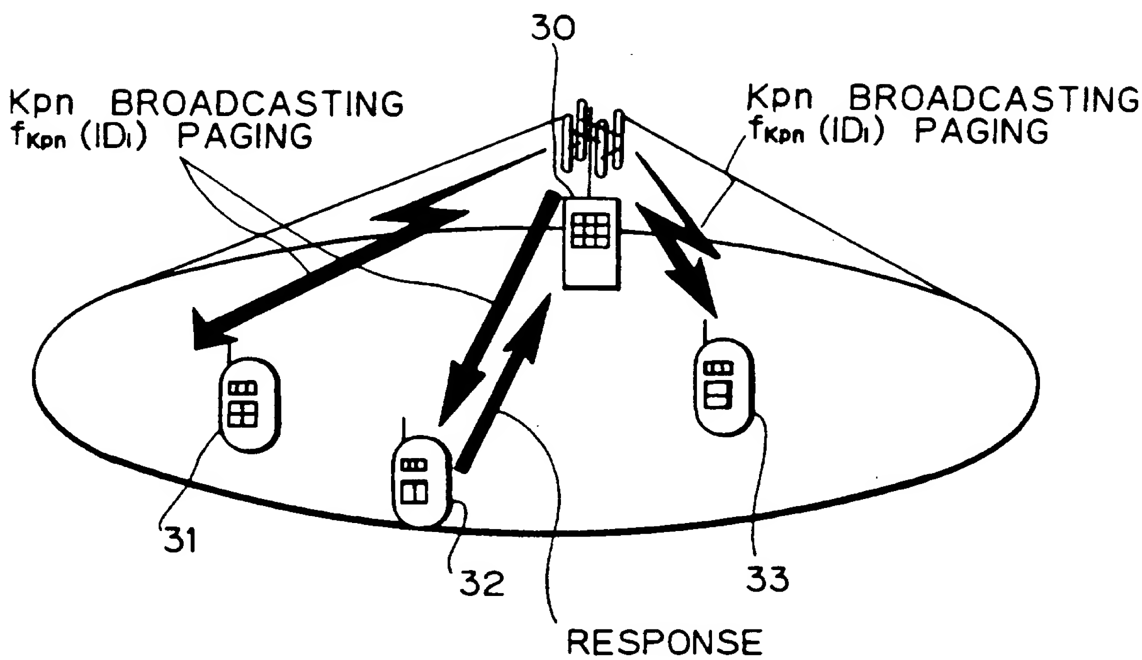

30
Kpn BROADCASTING
f_{Kpn} (ID_i) PAGING
Kpn BROADCASTING
f_{Kpn} (ID_i) PAGING
31
32
33
RESPONSE

Fig. 5

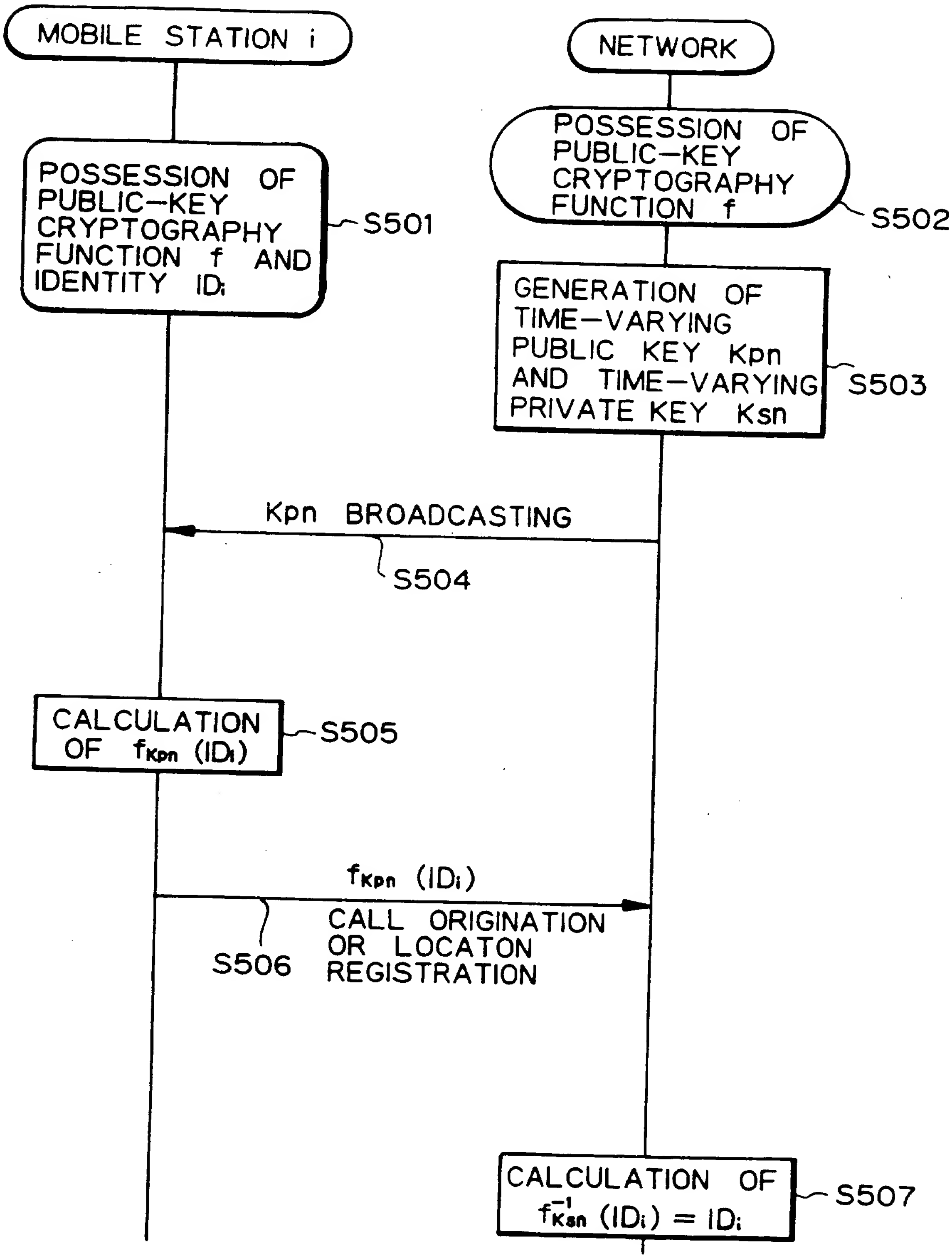

MOBILE STATION i
NETWORK
POSSESSION OF PUBLIC−KEY CRYPTOGRAPHY FUNCTION f AND IDENTITY ID_i
S501
POSSESSION OF PUBLIC−KEY CRYPTOGRAPHY FUNCTION f
S502
GENERATION OF TIME−VARYING PUBLIC KEY Kpn AND TIME−VARYING PRIVATE KEY Ksn
S503
Kpn BROADCASTING
S504
CALCULATION OF $f_{Kpn}(ID_i)$
S505
$f_{Kpn}(ID_i)$
CALL ORIGINATION OR LOCATON REGISTRATION
S506
CALCULATION OF $f^{-1}_{Ksn}(ID_i) = ID_i$
S507

Fig. 6

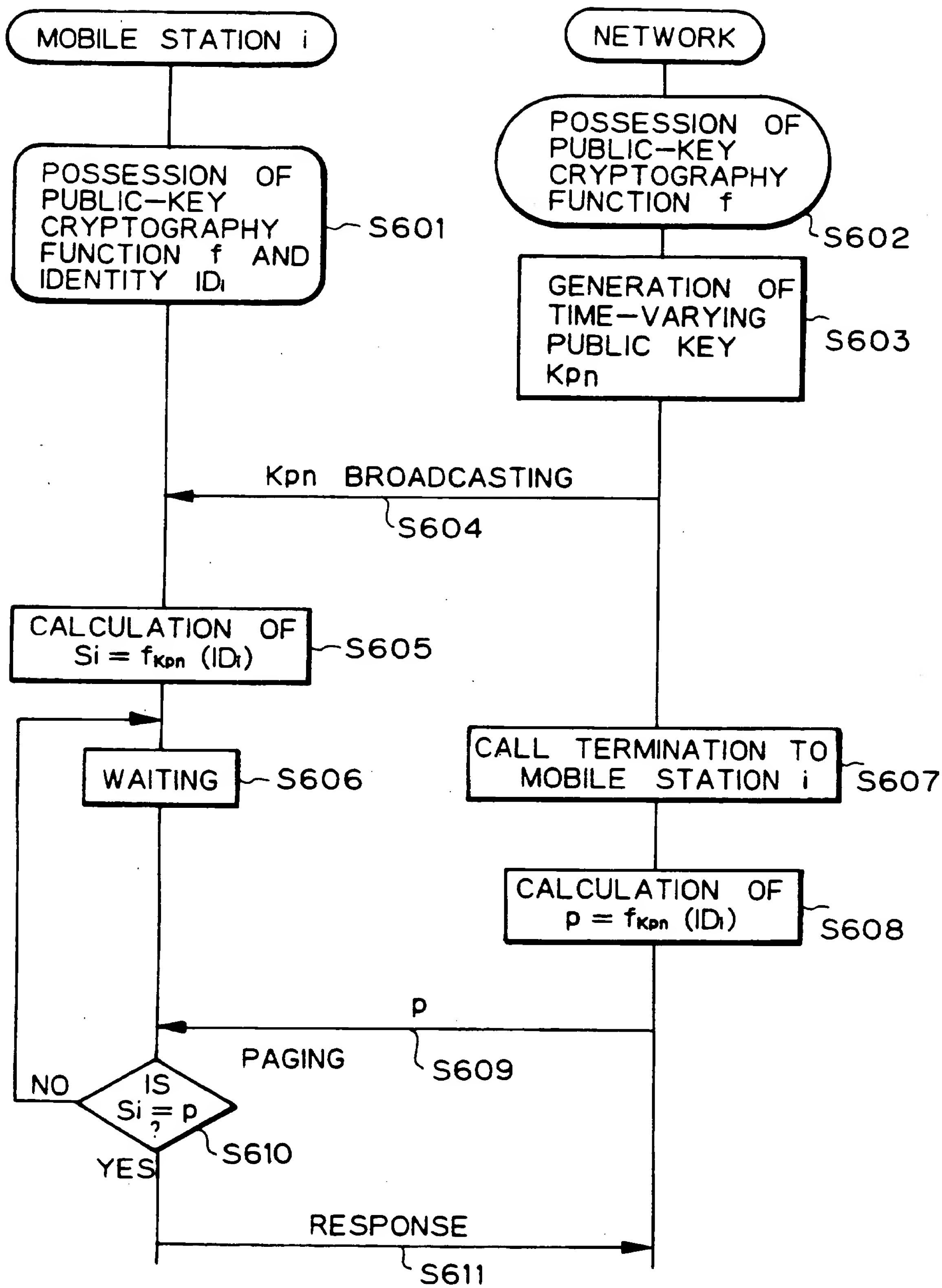
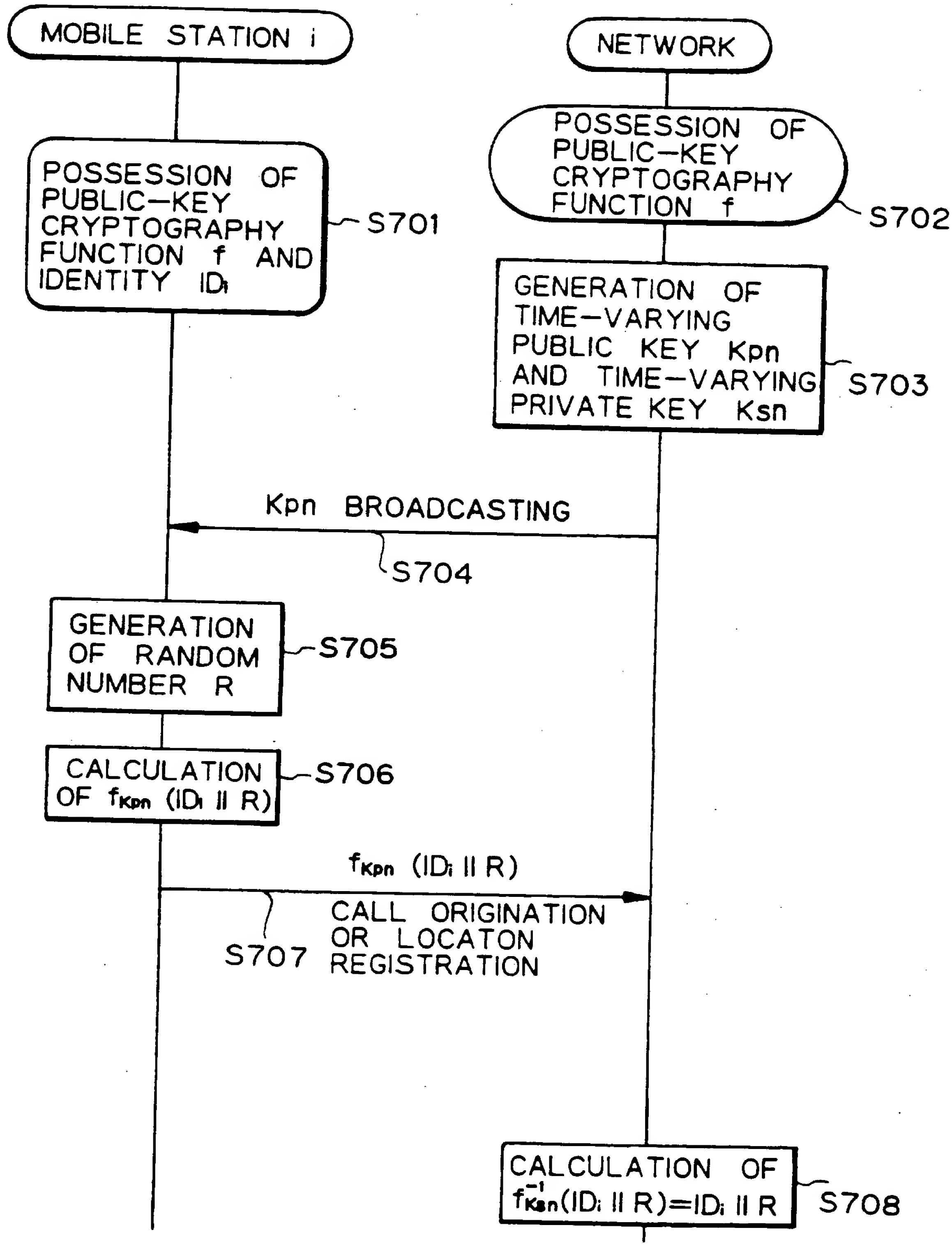

MOBILE STATION i
NETWORK
POSSESSION OF PUBLIC-KEY CRYPTOGRAPHY FUNCTION f AND IDENTITY ID_i
S601
POSSESSION OF PUBLIC-KEY CRYPTOGRAPHY FUNCTION f
S602
GENERATION OF TIME-VARYING PUBLIC KEY Kpn
S603
Kpn BROADCASTING
S604
CALCULATION OF $Si = f_{Kpn}(ID_i)$
S605
WAITING
S606
CALL TERMINATION TO MOBILE STATION i
S607
CALCULATION OF $p = f_{Kpn}(ID_i)$
S608
p
PAGING
S609
NO
IS $Si = p$?
YES
S610
RESPONSE
S611

Fig. 7


MOBILE STATION i
NETWORK
POSSESSION OF PUBLIC-KEY CRYPTOGRAPHY FUNCTION f AND IDENTITY IDi
S701
POSSESSION OF PUBLIC-KEY CRYPTOGRAPHY FUNCTION f
S702
GENERATION OF TIME-VARYING PUBLIC KEY Kpn AND TIME-VARYING PRIVATE KEY Ksn
S703
Kpn BROADCASTING
S704
GENERATION OF RANDOM NUMBER R
S705
CALCULATION OF f_{Kpn} (ID_i II R)
S706
f_{Kpn} (ID_i II R)
CALL ORIGINATION OR LOCATON REGISTRATION
S707
CALCULATION OF f^{-1}_{Ksn}(ID_i II R)=ID_i II R
S708

IDENTITY CONFIDENTIALITY METHOD IN RADIO COMMUNICATION SYSTEM

The present invention relates to an identity confidentiality method in a radio communication system. Particularly, the present invention relates to a method of keeping identity confidentiality in a mobile communication system, whereby elemental functions of network for mobile communication such as call origination, call termination and location registration can be securely performed by using identities encrypted so as to be indistinguishable from third parties in transit.

The radio transmission via a mobile communication network is more prone to eavesdropping than fixed wire transmission. For example, signal digits transmitted through radio paths can be easily received by third parties. Therefore, it is very important for the mobile communication to ensure security.

The security requirements to be ensured in the mobile communication consist of (1) protection against "masquerade", (2) security of communicating content, and (3) security of communicating location of a mobile station.

(1) protection against "masquerade"

This is a requirement for preventing unauthorized access to the network by a wrong mobile station who masquerades as a right mobile subscriber. To satisfy this requirement, (a) protection of subscriber identity (ID) against third-party tapping (ID confidentiality), and (b) authentication of an accessed mobile subscriber is necessary. Particularly, (b) is important for realizing this requirement.

(2) security of communicating content

This requirement is the most important for security. To satisfy this requirement, (c) enough confidentiality of communicating content by encryption against third-party listening is necessary.

(3) security of communicating location

This is a requirement for preventing mobile subscriber location from disclosure. To satisfy this requirement, (a) protection of subscriber identity against third-party tapping (ID confidentiality) is necessary.

Following is detail explanation of this (a) ID confidentiality.

For an identity to be transmitted on radio paths, it is the most defenseless to use a public number such as public telephone number without encryption. A mobile subscriber of this public telephone number will be directly specified by a third party. Some of existing mobile communication systems

have been kept at this security level. To use a secret telephone number as the identity without encryption is also defenseless because a third party can phone to a mobile subscriber of this secret telephone number. Usage of a public identity number without encryption is the same as the telephone number except that a third party cannot phone to a mobile subscriber of this public identity number.

Usage of a secret identity number will be more secure. However, the same number will be repeatedly used for accessing network, a wiretapper may specify the communicating mobile station from this accessed number. Thus, it has been recognized that usage of a temporary secret identity number is the most secure. Since this number is changed at every access or at necessary times, it is very difficult for wiretapper to specify the subscriber identity.

As a system using such temporary identity, there is GSM (Global System for Mobil communication) which has spread throughout Europe to worldwide. Hereinafter, temporary number-allocation in GSM will be described with reference to Figs. 1 and 2.

In GSM, a subscriber identity IMSI (International Mobile Subscriber Identity) which is secret even to its user is allocated to the user other than a telephone number. This allocated IMSI is stored into an IC card which is distributed to the user. Initially, a mobile station has no identity, but

after the IC card is inserted thereto, the IMSI stored in the card functions as an identity of this mobile station.

A home network possesses this IMSI as shown in Fig. 1 and always manages a location of the mobile station having this IMSI. When the mobile station initially accesses the GSM network, the IMSI is first transmitted from the mobile station via a radio path to a visited network (S101). Then, the visited network performs authentication process using a secret key cryptography algorithm so as to verify whether this mobile station is a legitimate user or not (S102-S104). If the mobile station is authenticated, the visited network registers the location of the mobile station (S105 and S106). Then, the visited network allocates a TMSI (Temporary Mobile Subscriber Identity) which is a kind of a penname to the mobile station (S107). The allocated TMSI is stored in a database in the visited network so that it can be referred to the corresponding IMSI (S112). Also, this allocated TMSI is ciphered and then the ciphered TMSI Ciph(TMSI) is transmitted via the radio path to the mobile station (S108 and S109). The mobile station deciphers the received cipher Ciph(TMSI) to extract TMSI (S110). The extracted TMSI is then stored in a memory of the IC card (S111). After that, all the accesses between this mobile station and the visited network such as call origination, call termination and location registration are executed by using this TMSI.

As shown in Fig. 2, in case that the mobile station moves to a new GSM network other than the network storing the above-mentioned TMSI, for example to a GSM network in the neighbor country, the mobile station informs the location of the previously visited network and the TMSI (hereinafter this previous TMSI is expressed as $TMSI_0$) via the radio path to the newly visited network (S201). The newly visited network inherits IMSI, TMSI, and authentication information etc. from the previously visited network (S202 and S203). The registered location information of this mobile station will be sent to the home network so as to renew its location information (S205). Then, the newly visited network may allocate a new TMSI to the mobile network (S206-S210), or may inherit the previous $TMSI_0$ for the mobile station.

When the mobile station in the visited network is called, this call is terminated to the visited network via the home network and then the mobile stations registered in this visited network are paged with the TMSI. The corresponding mobile station in the visited network responds to this call and will start communication after the authentication.

Thus, according to the GSM, ID confidentiality is performed by identifying a mobile station using the temporal identity of the TMSI.

Confidentiality itself is in general realized by means of encryption. There are two kinds of encryption, namely analog

encryption and digital encryption. Depending upon recent development of the digital mobile communication, the digital encryption has spread broader than the analog encryption.

The digital encryption is roughly divided into two cryptography systems, one a secret-key cryptography system and the other a public-key cryptography system.

The secret-key cryptography system (symmetric cryptosystem) which may be also called as a common-key cryptography system holds the same key at both ciphering and deciphering sides in common. Only users knowing this secret-key can cipher and decipher message. This secret-key cryptography has been widely used for confidentiality and authentication algorithms because the secret-key cipher is in general not so complicated and can be processed with high speed. Inner structures of many of secret-key cipher are kept in secret, but some of them are opened, known as for example DES or FEAL.

The public-key cryptography system (asymmetric cryptosystem) uses two different keys at ciphering and deciphering sides, respectively. One key used at the ciphering side is called as a public key and the other key used at the deciphering side is called as a private key. The public key is published while the private key is kept secret. Anyone can send a confidential message using the public key, but it cannot be deciphered without using a private key which is in the sole

possession of the intended receiver. Since the public key is based on mathematical algorithm such as factorization into prime factors, currently available public-key cryptography systems have a problem of low processing speed. Thus, this public-key encryption method is not so widely used in the mobile communication. As typical public-key cryptosystems, there are RSA (U.S. Patent No.4,405,829) and Rabin cipher for example. The basic ideas of public-key cryptography have been disclosed in U.S. Patent Nos.4,200,770 and 4,218,582.

Next, requirements for performing ID confidentiality in the mobile communication will be described.

Elemental functions of the network for mobile communication are, as aforementioned, location registration, call origination and call termination.

At the location registration, whether the mobile station to be registered is a legitimate subscriber is verified by presenting its identity and by performing the authentication. At the call origination, the same verification as that in the location registration will be executed in addition to a presentation of called subscriber number. The requirement for obtaining ID confidentiality at the location registration and the call origination is that no one except for the accessed network can specify the mobile subscriber in accordance with the received signal digits and therefore third parties cannot know who is accessing to the network.

At the call termination, it is necessary to perform paging operation. The requirement for obtaining ID confidentiality at the paging operation is that only the called mobile subscriber can confirm this call under the condition many of mobile subscribers in the cell are waiting for being called on the same radio channel. It is important that any mobile subscribers other than the called subscriber never recognize the paging identity and never mistake this call as a call directed to himself.

In order to satisfy these requirement of ID confidentiality, the aforementioned GSM using a temporal identity is advantageous because secure network control with the mobile station can be expected without always exposing the subscriber ID on the radio paths. However, according to the GSM, the IMSI has to be presented on the radio path when the mobile station initially accesses or when a trouble in the network occurs. Furthermore, in the GSM system, a great amount of network resources have to be utilized for managing the TMSI.

The ID confidentiality may be realized by encrypting the identity with a specific secret-key information determined by each user. For example, a confidential identity Si of a user i may be obtained by encrypting its identity IDi with the specific secret-key Ki determined by this user (mobile station) i. Namely, $Si=f_{Ki}(IDi)$. However, this ID confidentiality method using the specific secret-key information of each user

has following problems.

When the mobile station i actively accesses to the network due to for example the location registration or the call origination, only this confidential identity Si is directly presented to the network. As the network has in general no information with respect to any mobile stations accessed thereto except for this Si, it is quite difficult to decipher IDi from the received Si. Therefore, in order to perform this ID confidentiality method, it is necessary to have a memory table into which encrypted identities of all the mobile stations are previously stored. This will cause the network resources to greatly occupy as well as in case of possession of the TMSI.

When such the confidential identity Si is used for paging, it may be happened that a plurality of mobile stations are simultaneously called with the same Si. Namely, $f_{Ki}(IDi)=f_{Kj}(IDj)$ may occur for different mobile stations i and j ($i \neq j$), and thus a call for the mobile station i may be misjudged as a call for the mobile station j and vice versa. By appropriately designing, probability of occurrence of such error will be somewhat reduced but not to zero. In telephone communication, such problem as a plurality of terminals are simultaneously paged with one number never be admitted. The similar problems will occur during the call origination and the location registration.

Accordingly, the conventional ID confidentiality method using the specific information of each user cannot be well operated.

The ID confidentiality may also be realized by encrypting the identity with a specific information of the network. However, if the secret-key cryptography is used for the encryption, anyone who overhears the secret key in transit can know the identity encrypted using that key.

In accordance with one aspect of the present invention, a method of maintaining identity confidentiality in a radio communication system having at least one first radio station and a plurality of second radio stations, said first radio station at least possessing a public key, each of said second radio stations possessing a public-key cryptography function for ciphering the public key and an identity for identifying itself comprises the steps of: generating a time-varying public key at said first radio station; and repeatedly broadcasting, from said first radio station, the generated time-varying public key to all the second radio stations so that said second radio stations can cipher the respective identities with the broadcasted time-varying public key.

The present invention provides an identity confidentiality method in a radio communications system, whereby the identity can be securely and effectively hidden from anyone.

When the mobile station intends to originate a call or to register its location, this station ciphers his identity with the broadcasted public key and sends the encrypted identity to the base station. The base station receives this encrypted identity and deciphers it using a private key which is kept secret and corresponds to the public key, to obtain the identity. Thus, the identity can be securely provided to only the base station without being exposed to third parties.

Each of the mobile stations prepares in advance a ciphered identity by encrypting his identity with the time-varying public key and is waiting for being called. When a call to a mobile station is terminated, the base station ciphers the identify allocated to the called mobile station with the time-varying public key to obtain a ciphered identity and pages with this ciphered identity. The mobile station receives the paged and ciphered identity and compares the received ciphered identity with the previously prepared cip^ered identity. If both of the encrypted identifies coincide with each other, the mobile station recognizes the call termination and responds thereto. The mobile station to be called can only respond to the call termination without being known by eavesdropping third parties.

Furthermore, since the public key is time-varying, the encrypted result transmitted on the radio path becomes time-varying, which prevents from record and replay attacks. Thus, security of mobile communication can be greatly improved.

It is preferred that the base station further possesses a public-key cryptography function for ciphering the public key and a plurality of identities of the respective mobile stations, and that the method further includes steps of, at the mobile station, ciphering its identity with the broadcasted time-varying public key and waiting for a possible call thereto, and at the base station, ciphering the identity corresponding to a mobile station to be called with the time-varying public key and paging the ciphered identity to all the mobile stations.

It is also preferred that the base station further possesses a private key corresponding to the public key and a public-key cryptography function for deciphering a ciphered public key by using the private key, and that the method further includes steps of ciphering at one of the mobile stations the identity with the broadcasted time-varying public key and sending the ciphered identity to the base station, and receiving at the base station the ciphered identity sent from the at least one mobile station and deciphering the received ciphered-identity with the private key to extract the identity.

The ciphering and sending step may include steps of

generating a random number, combining the identity with the generated random number to provide a camouflaged identity, ciphering the camouflaged identity with the broadcasted time-varying public key, and sending the ciphered identity to the base station.

The receiving and deciphering step may include receiving at the base station the ciphered identity sent from the mobile station and deciphering the received ciphered-identity with the private key to extract the identity.

The receiving and deciphering step may further include a step of deciphering the received ciphered-identity with the private key and leaving a part of the random number from the deciphered result to extract the identity.

In another example, the radio communication system has at least one base station such as a base station and a plurality of mobile stations such as mobile stations. The base station at least possesses a one-way function f_K with a time-varying parameter k whereby for every x in the domain of f_K, $f_K(x)$ is easy to compute: but for virtually all y in the range of f, it is computationally infeasible to find an x such that $y=f_K(x)$. Each of the mobile stations possesses the same one-way function and an identity for identifying itself. In this case, the ——— method includes the steps of transferring, at the mobile station, its identity using the one-way function and

waiting for a possible call thereto, transferring, at the base station, the identity corresponding to a mobile station to be called using the one-way function, and paging the transferred identity to all the mobile stations.

Further objects and advantages of the present invention will be apparent from the following description of the preferred embodiments of the invention as illustrated in the accompanying drawings, in which:-

Fig. 1 is a flow chart showing the conventional ID confidentiality method in GSM already described;

Fig. 2 is a flow chart showing the another conventional ID confidentiality method in GSM already described;

Fig. 3 schematically illustrates operation of location registration / call origination according to the present invention;

Fig. 4 schematically illustrates operation of paging according to the present invention;

Fig. 5 is a flow chart showing operation of location registration / call origination of a preferred embodiment according to the present invention;

Fig. 6 is a flow chart showing operation of paging of the embodiment of Fig. 5; and

Fig. 7 is a flow chart showing operation of location

registration / call origination of an another embodiment according to the present invention.

In Fig. 3 which schematically illustrates operation of location registration / call origination according to the present invention, reference numeral 30 denotes a base station (network), and 31, 32 and 33 denote mobile stations, respectively. The network 30 always broadcasts a time-varying public key Kpn. When a mobile station i, for example the mobile station 32, intends to originate a call or to register its location, this station 32 ciphers his identity IDi with the public key Kpn and sends the encrypted identity $f_{Kpn}(IDi)$ to the network 30. The network 30 receives this $f_{Kpn}(IDi)$ and deciphers it using a private key Ksn, which is kept secret, corresponding to the public key Kpn to obtain the IDi.

Fig. 4 schematically illustrates operation of paging according to the present invention. The network 30 always broadcasts a time-varying public key Kpn. Each of the mobile stations 31, 32 and 33 prepares in advance $f_{Kpn}(ID)$ by encrypting his identity ID with the broadcasted time-varying public key Kpn and is waiting for being called. When a call to a mobile station i, for example to the mobile station 32, is terminated, the network 30 ciphers the identify IDi allocated to this station 32 with the time-varying public key Kpn to

obtain $f_{Kpn}(IDi)$ and pages with this ciphered $f_{Kpn}(IDi)$. The mobile station 32 receives the $f_{Kpn}(IDi)$ and compares the received $f_{Kpn}(IDi)$ with the previously prepared $f_{Kpn}(IDi)$. If both of the encrypted identifies coincide with each other, the mobile station 32 recognizes it is a call termination and responds thereto.

Fig. 5 is a flow chart showing operation when a mobile station confidentially sends his identity to a network due to for example location registration or call origination in a preferred embodiment according to the present invention.

The mobile station i possesses a public-key cryptography function f and an identify IDi allocated to himself in advance (S501). On the other hand, the network possesses the same public-key cryptography function f (S502). The network has a feature of generating a time-varying public key Kpn and a time-varying private key Ksn which corresponds to the public key Kpn (S503). This generation of the time-varying keys Kpn and Ksn is in this embodiment repeated at a predetermined time interval. The generated public key Kpn is repeatedly broadcasted (S504). The public key Kpn is thus published while the private key Ksn is kept secret.

When the mobile station i intends to originate a call or to register its location, this mobile station ciphers his own identity IDi with the broadcasted time-varying public key Kpn (S505) and sends the encrypted identity $f_{Kpn}(IDi)$ to the

network (S506). The network receives this f_{Kpn}(IDi) and deciphers it using the time-varying private key Ksn corresponding to the public key Kpn to extract the IDi (S507). Since the private key Ksn is kept secret except for this network, anyone who overhears f_{Kpn}(IDi) in transit cannot know the identify IDi. Furthermore, since the public key Kpn is time-varied, for example changed at a predetermined interval, the encrypted result f_{Kpn}(IDi) transmitted on the radio path becomes time-varying, which prevents from record and replay attacks. Thus, security of mobile communication can be greatly improved.

Fig. 6 is a flow chart showing operation of paging due to call termination in the embodiment of Fig. 5.

The mobile station i possesses the public-key cryptography function f and the identify IDi allocated to himself in advance (S601). On the other hand, the network possesses the same public-key cryptography function f (S602). The network has a feature of generating a time-varying public key Kpn, but is not necessary to generate a private key Ksn (S603). This generation of the time-varying public key Kpn is in this embodiment repeated at a predetermined time interval. The generated public key Kpn is always broadcasted (S604). The public key Kpn is thus published.

The mobile station i calculates in advance Si=f_{Kpn}(IDi) by encrypting his identity IDi with the broadcasted time-varying

public key Kpn each time this public key Kpn is updated (S605). Then, the mobile station i is waiting for being called (S606). When a call to a mobile station i is terminated, the network ciphers the identify IDi allocated to this mobile station i with the time-varying public key Kpn to obtain $p=f_{Kpn}(IDi)$ (S608), and pages with this p (S609). The mobile station i receives the p and compares the received p with the previously calculated Si (S610). If both of the encrypted identifies coincide with each other, namely if Si=p, the mobile station judges that he is called and sends a response to the network (S611). If it is not Si=p, the mobile station will return to the call-waiting state (S606). Any mobile stations except for this mobile station i cannot calculate the Si because they do not know the identity IDi. For the mobile stations other than the station i, the paged p will be looked like a random number. In other words, it is required that the allocated identity IDi has to be kept secret. Since the public key Kpn is time-varied, for example changed at a predetermined interval, the encrypted result $f_{Kpn}(IDi)$ transmitted on the radio path becomes time-varying, which prevents from record and replay attacks. Thus, security of mobile communication can be greatly improved.

It should be noted that, according to this ID confidentiality method, since different identities are mapped to different Si, there will never occur such problem as that a

plurality of users (mobile stations) are simultaneously called with the same Si.

As will be understood, in the aforementioned paging, deciphering calculation of the encrypted identity with the private key is not necessary. Therefore, instead of the above-mentioned public-key cryptography method, a cryptography using a one-way function f_K with a time-varying parameter k may be used whereby for every x in the domain of f_K, $f_K(x)$ is easy to compute: but for virtually all y in the range of f, it is computationally infeasible to find an x such that $y=f_K(x)$.

Fig. 7 is a flow chart showing operation when a mobile station confidentially sends his identity to a network due to for example location registration or call origination in an another embodiment according to the present invention.

The mobile station i possesses a public-key cryptography function f and an identify IDi allocated to himself in advance (S701). On the other hand, the network possesses the same public-key cryptography function f (S702). The network has a feature of generating a time-varying public key Kpn and a time-varying private key Ksn which corresponds to the public key Kpn (S703). This generation of the time-varying keys Kpn and Ksn is in this embodiment repeated at a predetermined time interval. The generated public key Kpn is repeatedly broadcasted (S704). The public key Kpn is thus published while the private key Ksn is kept secret.

When the mobile station i intends to originate a call or to register its location, this mobile station generates a random number R (S705) and combines his own identity IDi with this random number R to provide a camouflaged identity IDi‖R. Then, the mobile station ciphers this camouflaged identity IDi‖R with the broadcasted time-varying public key Kpn (S706) and sends the encrypted identity f_{Kpn}(IDi‖R) to the network (S707). The combination of the identity IDi with the random number R may be performed for example by adding a predetermined bits of the random number R after the last bit of the identity IDi.

The network receives this f_{Kpn}(IDi‖R) and deciphers it using the time-varying private key Ksn corresponding to the public key Kpn to extract the IDi‖R (S708). The identity IDi can be obtained by leaving the last predetermined bits of the extracted IDi‖R, which corresponds to the random number R. Since the private key Ksn is kept secret except for this network, anyone who overhears f_{Kpn}(IDi‖R) in transit cannot know the camouflaged identify IDi‖R, and therefore the identity IDi. Furthermore, since the public key Kpn is time-varied, for example changed at a predetermined interval and IDi‖R is always variable, the encrypted result f_{Kpn}(IDi‖R) transmitted on the radio path is always variable on each access, which prevents from record and replay attacks. In this case, the public key Kpn may not be time-varying since the random number R makes the

encrypted result variable. Thus, security of mobile communication can be greatly improved.

CLAIMS

1. A method of maintaining identity confidentiality in a radio communication system having at least one first radio station and a plurality of second radio stations, said first radio station at least possessing a public key, each of said second radio stations possessing a public-key cryptography function for ciphering the public key and an identity for identifying itself, said method comprising the steps of:

generating a time-varying public key at said first radio station; and

repeatedly broadcasting, from said first radio station, the generated time-varying public key to all the second radio stations so that said second radio stations can cipher the respective identities with the broadcasted time-varying public key.

2. The method as claimed in claim 1, wherein said first radio station further possesses a public-key cryptography function for ciphering the public key and a plurality of identities of the respective second radio stations, and wherein said method further comprises steps of, at the second radio station, ciphering its identity with the broadcasted time-varying public key and waiting for a possible call thereto, and at the first radio station, ciphering the identity corresponding to a second

radio station to be called with the time-varying public key and paging the ciphered identity to all the second radio stations.

3. The method as claimed in claim 2, wherein said first radio station further possesses a private key corresponding to the public key, and a public-key cryptography function for deciphering a ciphered public key by using the private key, and wherein said method further comprises steps of ciphering at one of the second radio stations the identity with the broadcasted time-varying public key and sending the ciphered identity to the first radio station, and receiving at the first radio station the ciphered identity sent from the at least one second radio station and deciphering the received ciphered-identity with the private key to extract the identity.

4. The method as claimed in claim 3, wherein said ciphering and sending step includes steps of generating a random number, combining the identity with the generated random number to provide a camouflaged identity, ciphering the camouflaged identity with the broadcasted time-varying public key, and sending the ciphered identity to the first radio station.

5. The method as claimed in claim 4, wherein said receiving and deciphering step includes receiving, at the first radio station, the ciphered identity sent from the second radio

station and deciphering the received ciphered-identity with the private key to extract the identity.

6. The method as claimed in claim 5, wherein said receiving and deciphering step further includes a step of deciphering the received ciphered-identity with the private key and leaving a part of the random number from the deciphered result to extract the identity.

7. A method of maintaining identity confidentiality in a radio communication system having at least one first radio station and a plurality of second radio stations, said first radio-station possessing a public key, a private key corresponding to the public key, and a public-key cryptography function for deciphering a ciphered public key by using the private key, each of said second radio stations possessing a public-key cryptography function for ciphering the public key and an identity for identifying itself, said method comprising the steps of:

generating a time-varying public key at said first radio station;

repeatedly broadcasting, from said first radio station, the generated time-varying public key to all the second radio stations;

ciphering at one of the second radio stations the identity

with the broadcasted time-varying public key and sending the ciphered identity to the first radio station; and

receiving at the first radio station the ciphered identity sent from the at least one second radio station and deciphering the received ciphered-identity with the private key to extract the identity.

8. The method as claimed in claim 7, wherein said ciphering and sending step includes steps of generating a random number, combining the identity with the generated random number to provide a camouflaged identity, ciphering the camouflaged identity with the broadcasted time-varying public key, and sending the ciphered identity to the first radio station.

9. The method as claimed in claim 8, wherein said receiving and deciphering step includes receiving, at the first radio station, the ciphered identity sent from the second radio station and deciphering the received ciphered-identity with the private key to extract the identity.

10. The method as claimed in claim 9, wherein said receiving and deciphering step further includes a step of deciphering the received ciphered-identity with the private key and leaving a part of the random number from the deciphered result to extract the identity.

11. A method of maintaining identity confidentiality in a radio communication system having at least one first radio station and a plurality of second radio stations, said first radio station possessing a one-way function f_K with a time-varying parameter k whereby for every x in the domain of f_K, $f_K(x)$ is easy to compute but for virtually all y in the range of f, it is computationally infeasible to find an x such that $y=f_K(x)$, said one-way function being capable of using a time-varying parameter, each of said second radio stations possessing the same one-way function and an identity for identifying itself, said method comprising the steps of:

generating a time-varying parameter at said first radio station;

repeatedly broadcasting, from said first radio station, the generated time-varying parameter to all the second radio stations so that said second radio stations can cipher the respective identities with the broadcasted time-varying parameter;

transferring, at the second radio station, its identity using said one-way function and waiting for a possible call thereto;

transferring, at the first radio station, the identity corresponding to a second radio station to be called using said one-way function; and

paging the transferred identity to all the second radio stations.

12. A method of maintaining identity confidentiality in a radio communication system substantially as hereinbefore described with reference to any of the examples shown in Figures 3 to 7 of the accompanying drawings.

13. A radio communication system adapted to operate an identity confidentiality method according to any of the preceding claims.

The Patent Office

28

Application No: GB 9525817.4
Claims searched: 1-13

Examiner: Mr B J Spear
Date of search: 4 March 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4P (PDCSA, PDCSC)

Int Cl (Ed.6): H04L 9/30, 9/32

Other: Online: WPI, Claims, Inspec

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	US5222140	(Bell Comms. Research) Whole document, eg, col. 7 line 58-col. 9 line 50.	1,2,7,11 and 13

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.